Iwona Banaszek

MASZYNY SZYFRUJĄCE II WOJNY ŚWIATOWEJ

Enigma - niemiecka przenośna maszyna szyfrująca opracowana przez Hugo Kocha, który sprzedał patent rozwiązań wykorzystanych przy jej budowie inżynierowi Arturowi Scherbiusowi, a ten z kolei wraz z Richardem Ritterem założył firmę produkującą maszyny szyfrujące Scherbius & Ritter.



Enigma była używana komercyjnie od lat 20. XX wieku, a później została zaadaptowana przez instytucje państwowe wielu krajów. Podczas II wojny światowej maszyna ta była wykorzystywana głównie przez siły zbrojne oraz inne służby państwowe i wywiadowcze Niemiec, ale także innych państw. Enigma należała do rodziny elektromechanicznych wirnikowych maszyn szyfrujących i była produkowana w wielu różnych odmianach.

Najczęściej odszyfrowywanymi wiadomościami były przekazy zaszyfrowane Enigmą w wersji Wehrmachtu (Wehrmacht Enigma). Brytyjski wywiad wojskowy oznaczył Enigmę kryptonimem ULTRA. Nazwa ta powstała ze względu na najwyższy stopień utajnienia faktu złamania szyfru Enigmy, wyższy niż najtajniejszy (ang. Most Secret), czyli Ultra tajny.

Historia Enigmy jako niemieckiego systemu łączności szyfrowej zaczęła się w latach 1926-28, kiedy w niemieckich służbach wprowadzono automatyczne urządzenia szyfrujące. Jeszcze przed dojściem Hitlera do władzy, w 1932 roku chciano stworzyć liczniejszą armię. Rozbudowa wojsk szybkich i lotnictwa mogących posłużyć w „wojnie błyskawicznej" wymagała niezawodnych środków szyfrowania. Z czasem wszystkie niemieckie siły zbrojne oraz dowództwa, od Kwatery Głównej Hitlera po dywizje pułki i brygady zostały wyposażone w maszyny Enigma. Na frontach II wojny światowej działało prawdopodobnie ponad 100 tys. takich urządzeń. Po wojnie były one niszczone przez aliantów, część z nich zaś sprzedano, gdyż popyt na nie był duży. Może właśnie dlatego tak długo złamanie tego kodu owiane było tajemnicą. Do dziś zachowało się prawdopodobnie kilka egzemplarzy Enigmy. Jeden z nich został przekazany Polsce przez brytyjskiego księcia Andrzeja.

Duże zainteresowanie Enigmą pojawiło się w Europie w latach 70-tych. Gustav Bertrand, były szef francuskiego radiowywiadu, który blisko współpracował z wywiadem polskim za czasów II wojny światowej, w swej książce z 1973 roku ujawnił fakt, iż niemiecki szyfr złamali alianci, a kluczową rolę odegrali Polacy. Nie on pierwszy jednak o tym wspominał, jak się powszechnie uważa, gdyż kilka lat wcześniej pisał już o tym Władysław Kozaczuk („Bitwa o tajemnice"). Rok później, w publikacji F.W. Winterbothama „The Ultra Secret" (bowiem Enigma w Anglii nazywana była Ultra) znaczenie Polaków zostało zupełnie zredukowane. Autor wspomina jedynie o „jakimś" polskim mechaniku zatrudnionym w Niemczech przy budowie maszyn szyfrujących. Wywołało to dyskusje, czy w ogóle nasi rodacy uczestniczyli w tym przedsięwzięciu.

Po raz pierwszy poza Polską w 1974 roku, w USA zostały podane nazwiska polskich autorów matematycznego rozwiązania Enigmy.

Polscy łamacze szyfrów

Już na przełomie lat 20-tych i 30-tych XX wieku Polacy próbowali złamać kod Enigmy. W tym czasie oficerowie Sztabu Głównego Wojska Polskiego zorganizowali kurs kryptologii dla wybranych studentów matematyki Uniwersytetu Poznańskiego, co miało pozostać tajemnicą. Uczestniczyli w nim m.in. trzej późniejsi łamacze szyfrów – **Marian Rejewski**, **Henryk Zygalski** i **Jerzy Różycki**, którzy potrafili pogodzić kurs szyfrów i obowiązki studentów.

Jako pierwszy Enigmą zajął się Rejewski, dzięki któremu w 1933 roku zbudowano replikę tej maszyny. Samo posiadanie jej nie pozwoliło odczytywać zaszyfrowanych wiadomości, jednak Polacy próbowali złamać tajemniczy kod, a ułatwiały im to pomyłki samych szyfrantów. W 1933 roku nasi rodacy odczytywali komunikaty niemieckie. Sukces przyszedł w samą porę, gdyż w Niemczech dokonywał się przewrót, który 30 stycznia 1933 roku oddał władzę w ręce Hitlera. Po kilku latach, w czasie których znacznie polepszyło się szyfrowanie, odczyt rozkazów stał się dużo trudniejszy, szczególnie po 15 września 1938 roku. W lipcu 1939 roku, tuż przed atakiem na nasz kraj, polscy kryptolodzy spotkali się w Warszawie z przedstawicielami Francji oraz Wielkiej Brytanii i przekazali im zrekonstruowaną Enigmę, a także wszelkie materiały na temat sposobu kodowania. Brytyjczycy byli osłupieni wynikami działań polskich specjalistów i po raz pierwszy musieli uznać ich wyższość. Skorzystali oni z owoców 8-letniej francusko-polskiej przyjaznej współpracy. W ostatnie dni sierpnia 1939 roku trwały gorączkowe prace w Biurze Szyfrów. Wprowadzono całodobowe dyżury kryptologów. W wyniku działań wojennych kryptolodzy polscy musieli ewakuować się do innych krajów.

Losy trzech matematyków

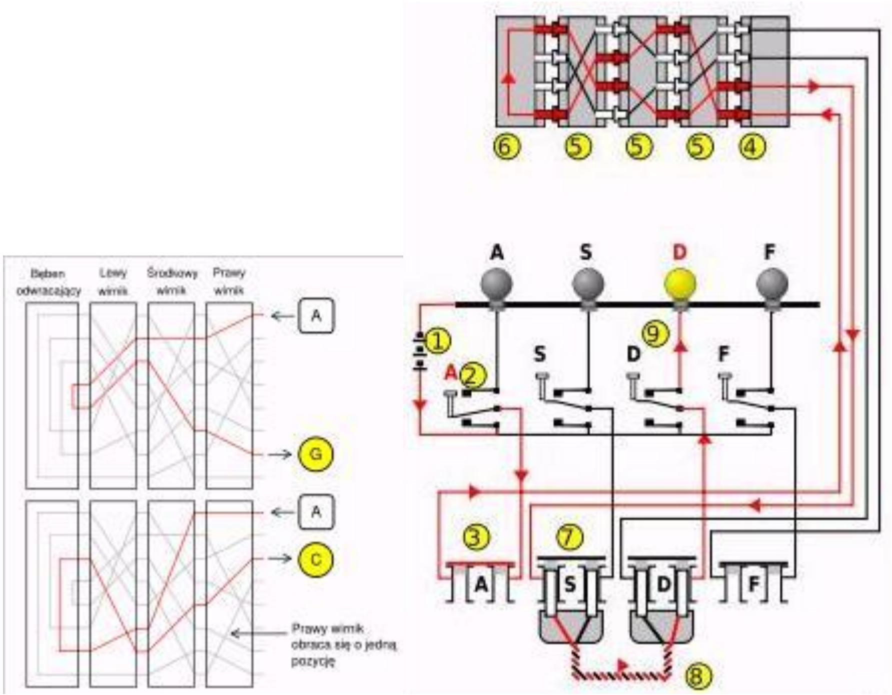
Marian Rejewski (1905-1980), urodzony w Bydgoszczy, pracował jako asystent na Uniwersytecie Poznańskim, po czym przeniósł się do Biura Szyfrów w Warszawie. Po wojnie, w roku 1946, jako jedyny z trójki Polaków wrócił do ojczyzny, do żony i dwójki dzieci. W 1967 roku napisał wspomnienia z pracy w Biurze Szyfrów, ukazując prawdę o złamaniu Enigmy. Zdeponował je w Wojskowym Instytucie Historycznym, jednak nie doczekały się wydania. Zmarł w Warszawie.

Henryk Zygalski (1907-1978), urodzony w Poznaniu, po zakończeniu wojny pozostał na zawsze w Wielkiej Brytanii. Pracował tam w polskim collage’u. Uwielbiał grać na fortepianie. Zmarł w Plymouth.

Jerzy Różycki (1909-1942), urodzony w Olszanach na Kijowszczyźnie, w Poznaniu prócz matematyki studiował jeszcze geografię. Z powodu wojny, podobnie jak poprzednicy, musiał opuścić kraj, a w nim żonę i kilkumiesięczne dziecko. Ten najmłodszy z polskich kryptologów zginął w czasie wojny. Utonął w okolicach Balearów w katastrofie statku, który w styczniu 1942 roku wracał z rejsu do Algieru.

W Pyrach pod Warszawą, w miejscu, gdzie Polacy przekazali aliantom dane o sposobie kodowania Enigmy, znajduje się tablica pamiątkowa, na której wypisane są nazwiska w/w kryptologów. Również w Bletchley Park ma się pojawić tablica im poświęcona.

Opis działania



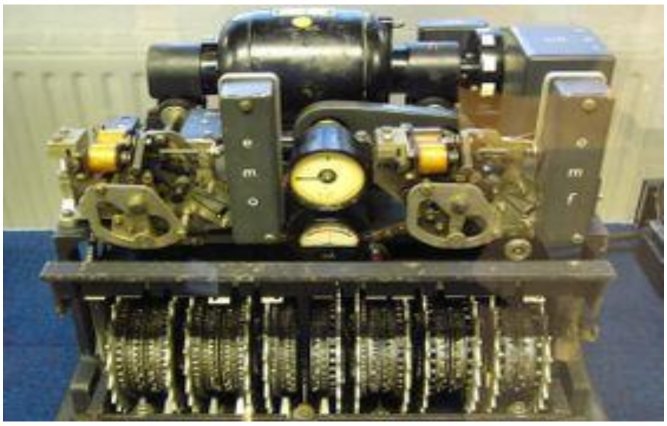
Tak jak inne maszyny oparte na rotorach Enigma jest połączeniem systemów elektrycznego i mechanicznego. Część mechaniczna składa się z alfabetycznej 26 znakowej klawiatury, zestawu osadzonych na wspólnej osi i obracających się bębenków nazywanych rotorami lub wirnikami (niem. Chiffrierwalzen) oraz mechanizmu obracającego jeden lub kilka rotorów na raz za każdym naciśnięciem klawisza.

Części mechaniczne służą jako elementy obwodu elektrycznego - właściwe kodowanie liter odbywa się elektrycznie. Po naciśnięciu klawisza obwód elektryczny zamyka się, a prąd przepływa przez elementy składowe maszyny ostatecznie powodując zapalenie się jednej z wielu lampek podświetlających literę wyjściową. Na przykład, jeśli kodowana wiadomość zaczyna się od liter ALA..., operator maszyny naciska najpierw literę A, która może spowodować zapalenie się lampki z literą Z. W ten sposób pierwszą literą zakodowanej wiadomości będzie Z. Następnie operator naciska klawisz z literą L, która zostaje zakodowana w analogiczny sposób i tak dalej.

Prace nad Enigmą prowadzone były również w Wielkiej Brytanii, w Bletchley Park, jednak tam Polacy nie zostali zaproszeni do współpracy. To centrum dekryptażu rozpoczęło działalność w 1938 roku, podczas wojny nazywane było Stacją X. Pracowali tam najlepsi brytyjscy matematycy (np. Alan Turing), lingwiści i inżynierowie oraz agenci wywiadu. Bletchley Park uznawane jest za kolebkę informatyki. Choć zatrudnionych było tam kilkanaście tys. osób, to nie znali oni szczegółów akcji. Poza tym cały ośrodek owiany był tajemnicą, a o jego istnieniu opinia publiczna dowiedziała się dopiero w latach 70-tych.

Powszechnie uważa się, iż dopiero w Bletchley Park rozpoczęły się działania prowadzące do rozkodowania Enigmy, lecz wiedza Polaków była dla Brytyjczyków bezcenna i bez niej alianci nie zdołaliby odczytać tajnych niemieckich depesz przed bitwą o Atlantyk.

Maszyna Lorenza (Lorenz-Chiffre, Schlüsselzusatz; Lorenz SZ 40 i SZ 42) - niemiecka maszyna szyfrująca używana podczas II wojny światowej dla przekazu informacji przez dalekopisy. Brytyjscy analitycy, którzy zakodowane komunikaty dalekopisowe określali kodem "Fish" (ryba), szyfry maszyny Lorenza i ją samą nazywali "Tunny" (tuńczyk). O ile słynna Enigma była używana przez jednostki polowe, o tyle Tunny służyła do komunikacji wysokiego szczebla, gdzie można było wykorzystać ciężką maszynę, dalekopis i dedykowane łącza. Maszyna Lorenza przypominała Enigmę ponieważ również korzystała z rotorów, lecz działała na innej zasadzie. Miała wymiary 51 cm × 46 cm × 46 cm i stanowiła przystawkę do standardowego dalekopisu Lorenza. Z punktu widzenia kryptografii, implementowała szyfr strumieniowy.



Opis działania

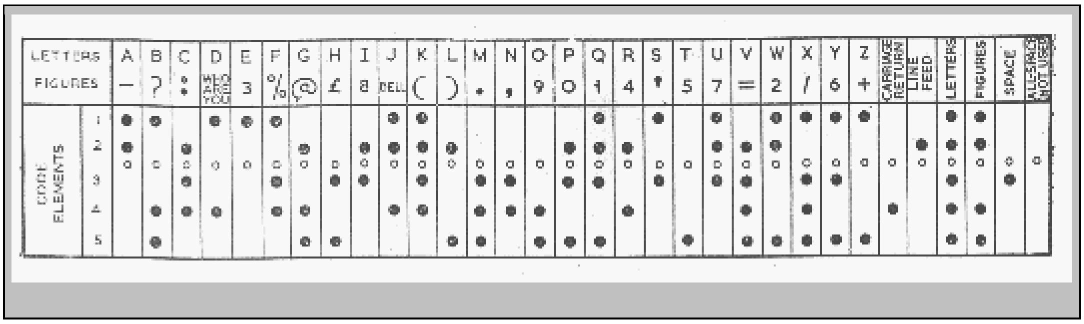
Ówczesne dalekopisy nadawały każdą literę, ogólnie zaszyfrowaną kodem Baudot albo podobnym, jako pięć bitów na pięciu równoległych liniach. Maszyna Lorenza

produkowała grupę pięciu bitów pseudolosowych i kombinowała ją za pomocą logicznego operatora XOR z bitami litery tekstu jawnego. Bity pseudolosowe były generowane przez 10 "kół kryptograficznych" (rotorów), z których pięć obracało się w sposób regularny (tzw. koła chi) a pięć pozostałych w sposób nieregularny (koła psi). Krok obrotu kół psi zależał od jeszcze dwóch dodatkowych rotorów, zwanych motorycznymi (napędowymi). Maszyna Lorenza w swej funkcji nieregularnego obracania pięciu rotorów (które albo razem się obracały albo razem pozostawały w spoczynku bez dodatkowych interakcji między liniami) stanowi w praktyce 5 równoległych generatorów pseudolosowych. Liczby igieł na każdym z rotorów były względnie pierwsze.

Niemiecki system szyfrowania Lorenz

Naczelne Dowództwo Niemieckiej Armii zwróciło się do firmy Lorenz o wyprodukowanie dla niego maszyny szyfrującej kod dalekopisowy o wysokim bezpieczeństwie w celu umożliwienia całkowicie tajnej komunikacji radiowej. Firma Lorenz zaprojektowała maszynę szyfrową opartą na addytywnej metodzie szyfrowania wiadomości dalekopisowych wynalezionej w 1918 przez Gilberta Vernama w Ameryce.

Dalekopisy nie opierają się na 26 literowym alfabecie i kodzie Morse'a, od których zależała Enigma. Dalekopisy używają 32 znakowego kodu Baudota. Zwróć uwagę, że kod ten składa się z pięciu kanałów, z których każdy jest strumieniem bitów mogących być przedstawionymi jako dziurka lub jej brak na taśmie perforowanej, 0 lub 1, kropka lub krzyżyk.



System Vernama szyfrował tekst wiadomości przez dodanie do niej znak po znaku zbioru zasłaniających znaków, wytwarzając w ten sposób zaszyfrowane znaki, które były transmitowane do zamierzonego odbiorcy. Prostota systemu Vernama polegała na tym, iż zasłaniające znaki były dodawane w dosyć specjalny sposób (znany jako dodawanie modulo 2). Następnie dokładnie te same znaki zasłaniające dodane modulo 2 do odebranych znaków

zaszyfrowanych powodowały wydobycie oryginalnej wiadomości, która mogła dalej zostać wydrukowana.

Działanie dodawania modulo 2 jest dokładnie takie samo jak logiczna operacja XOR:

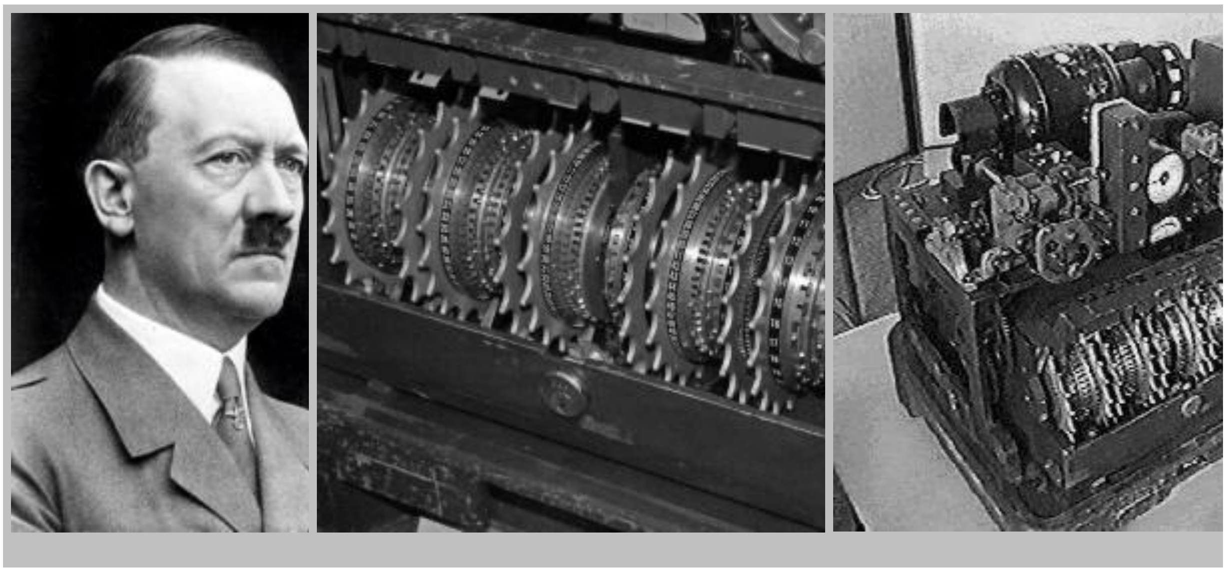
0 XOR 0 = 0
0 XOR 1 = 1
1 XOR 0 = 1
1 XOR 1 = 0

Jeśli A jest literą tekstu jawnego, a C jest znakiem zasłaniającym, to zgodnie z poniższym rachunkiem literą szyfru jest F. Z rachunku możesz również zobaczyć, że dodanie C do F daje z powrotem A:

A + C = F	F + C = A
1 + 0 = 1	1 + 0 = 1
1 + 1 = 0	0 + 1 = 1
0 + 1 = 1	1 + 1 = 0
0 + 1 = 1	1 + 1 = 0
0 + 0 = 0	0 + 0 = 0

Vernam proponował, aby zasłaniające znaki były zupełnie przypadkowe i wydziurkowane wcześniej na papierowej taśmie, która byłaby zużywana znak po znaku synchronicznie ze znakami wprowadzanej wiadomości. Taki system szyfrowania (jednorazowy) używający *czysto losowych* znaków zasłaniających jest nie do złamania.

Trudność polegała na zapewnieniu, iż w warunkach wojennych te same taśmy z przypadkowymi znakami będą dostępne po obu końcach połączenia komunikacyjnego i że obie zostaną ustawione na tę samą pozycję startową. Firma Lorenz zdecydowała, że będzie pod względem operacyjnym prościej zbudować maszynę generującą ciąg znaków zasłaniających. Ponieważ była to maszyna, to nie mogła tworzyć zupełnie przypadkowego ciągu znaków. Tworzył ciąg znany jako ciąg pseudolosowy. Na nieszczęście dla Niemieckiej Armii był on bardziej "pseudo" ni losowy i dlatego właśnie został złamany.



Zabawną rzeczą na temat maszyny Lorenz było to, że łamacze szyfrów z Bletchley Park nigdy nie widzieli rzeczywistej maszyny Lorenz aż do zakończenia działań wojennych, lecz łamali jej szyfry już od dwóch i pół roku.

Pierwsze przechwycenia wiadomości

Sygnały dalekopisowe wysyłane przez Niemców i szyfrowane maszyną Lorenz zostały po raz pierwszy usłyszane na początku roku 1940 przez grupę policjantów z Południowego Wybrzeża, którzy prowadzili nasłuch możliwych transmisji niemieckich szpiegów z terenu Anglii. Brygadier John Tiltman, jeden z głównych łamaczy szyfrów w Bletchley Park, zainteresował się szczególnie tymi zaszyfrowanymi wiadomościami dalekopisowymi. Nadano im nazwę kodową "Fish" (ryba). Wiadomości, które (jak odkryto później) były szyfrowane za pomocą maszyny Lorenz, znano pod nazwą "Tunny" (tuńczyk). Tiltman znał system Vernama i wkrótce zidentyfikował te wiadomości jako szyfrowane na sposób Vernama.

Ponieważ system Vernama polegał na dodawaniu znaków, Tiltman doszedł do wniosku, że jeśli operatorzy popełnią błąd i użyją tych samych ustawień początkowych maszyny Lorenz dla dwóch wiadomości (głębokość), to poprzez dodanie do siebie takich dwóch zaszyfrowanych tekstów znak po znaku ciąg znaków zasłaniających zniknie. Otrzymałby wtedy ciąg znaków, z których każdy reprezentował by sumę dwóch odpowiadających sobie znaków w oryginalnych niemieckich tekstach wiadomości. Dla dwóch zupełnie różnych wiadomości praktycznie nie jest możliwe przypisanie właściwych znaków każdej z nich.

Tylko niewielkie fragmenty na początku mogły być odtworzone, lecz nie kompletne wiadomości.

Niemiecka pomyłka

Gdy wzrosła liczba przechwytywanych wiadomości przez jednostkę w Knockholt w Kent, w Bletchley Park stworzono nowy oddział, którego kierownictwem zajął się major Ralph Tester - oddział ten znany był jako Testery. Przechwycono pewną liczbę wiadomości, lecz nie było dużego postępu w złamaniu tego kodu aż do momentu, gdy Niemcy popełnili horrendalny błąd. Wydarzyło się to 30 sierpnia 1941. Pewien niemiecki operator musiał przesłać długi ciąg prawie 4000 liter z jednej części Niemieckiego Naczelnego Dowództwa do drugiej - prawdopodobnie z Aten do Wiednia. Prawidłowo ustawił maszynę Lorenz a następnie wysłał, wykorzystując niemieckie imiona, dwunastoliterowy indykator do operatora na drugim końcu połączenia. Ten operator ustawił swoją maszynę Lorenz i poprosił operatora nadającego o rozpoczęcie nadawania wiadomości. Po wprowadzeniu ręcznie prawie 4000 znaków operator odbierający wysłał z powrotem przez radio wiadomość po niemiecku "nie dostałem tego - wyślij jeszcze raz".

Teraz obaj ustawili swoje maszyny Lorenz z powrotem w tej samej pozycji startowej. Było to absolutnie zakazane, ale zrobili to. Następnie operator nadający rozpoczął ponowne ręczne wpisywanie wiadomości. Gdyby był on robotem u użył dokładnie tych samych naciśnięć klawiszy jak za pierwszym razem, to nasłuchowcy mieliby jedynie dwie identyczne kopie tej samej zaszyfrowanej wiadomości. Jeśli na wejściu maszyny jest ten sam tekst, to maszyna, generując takie same znaki przesłaniające, tworzy ten sam szyfr. Lecz będąc tylko człowiekiem oraz wkurzywszy się na myśl o powtórnym wklepaniu tej samej wiadomości, operator wysyłający zaczął tworzyć różnice w drugiej wiadomości w porównaniu z pierwszą.

Wiadomość rozpoczynała się od dobrze znanego niemieckiego wyrażenia SPRUCHNUMMER - "numer wiadomości". Za pierwszym razem operator ten wpisał SPRUCHNUMMER. Za drugim razem wpisał SPRUCHNR i dalej resztę tekstu wiadomości. Teraz NR znaczyło to samo co NUMMER, zatem jaką robiło to różnicę? Oznaczało to, że bezpośredni za N oba teksty były różne. Lecz maszyna generowała ten sam ciąg zasłaniających znaków, dlatego oba teksty różniły się począwszy od tego miejsca.

Nasłuchowcy w Knockholt zdali sobie sprawę z możliwej wagi tych dwóch wiadomości, ponieważ dwunastoliterowe indykatory były takie same. Wysłano je pocztą ekspresową do

Johna Tiltmana w Bletchley Park. Tiltman zastosował na tej parze tę samą addytywną technikę, którą stosował na poprzednich Głębokościach. Lecz tym razem był w stanie pójść o wiele dalej w rozpracowaniu rzeczywistego tekstu wiadomości, ponieważ po użyciu SPRUCHNUMMER na początku, natychmiast zauważył, że druga wiadomość była prawie identyczna z pierwszą. W ten sposób połączone błędy związane z ponownym ustawieniem maszyn na tej samej pozycji startowej oraz ponownym przesłaniu tekstu z małymi różnicami pozwoliły Tiltmanowi odtworzyć całkowicie oba teksty. Drugi był około 500 znaków krótszy od pierwszego, ponieważ niemiecki operator oszczędzał swoje palce. Ten fakt również pozwolił Tiltmanowi przypisać właściwą wiadomość do jej oryginalnego tekstu szyfrowego.

Teraz Tiltman mógł dodać razem znak po znaku odpowiednie szyfry i teksty wiadomości otrzymując po raz pierwszy długi ciąg zasłaniających znaków generowanych przez niemiecką maszynę szyfrującą. Nie wiedział jak to ta maszyna zrobiła, lecz wiedział, że to właśnie generowała!

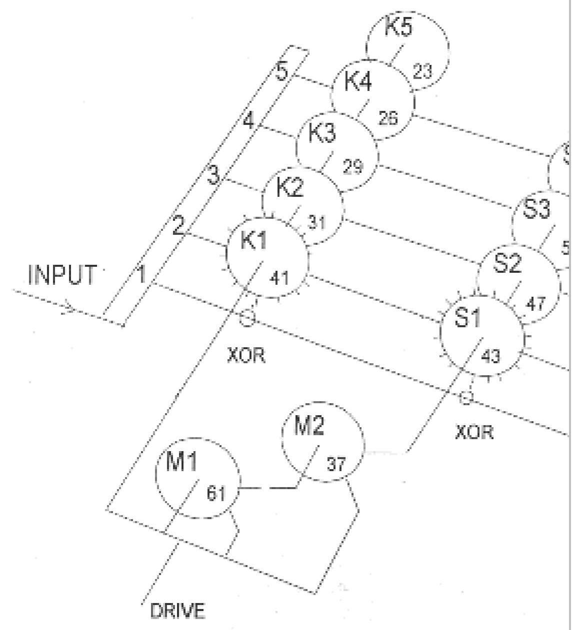
Rozwiązanie zagadki

John Tiltman dał swój długi ciąg zasłaniających znaków młodemu absolwentowi chemii, Billowi Tutte, który niedawno przyszedł do Bletchley Park z Cambridge. Bill Tutte zaczął wypisywać wzory bitowe z każdego z pięciu kanałów w postaci dalekopisowej tego ciągu znaków przesłaniających przy różnych okresach powtarzania. Było to przed erą komputerów i wszystko musiał zapisywać ręcznie w długich sekwencjach.

Gdy wypisał wzory bitowe z kanału 1 z okresem powtarzania 41, to zaczęły się wyłaniać różne prawidłowości, które nie były takie przypadkowe. Pokazało to, że okres powtarzania 41 posiadał jakieś znaczenie w metodzie generowania tego szyfru. Następnie przez ponad dwa kolejne miesiące Tutte wraz z innymi członkami sekcji Badań rozpracowali kompletną strukturę logiczną maszyny szyfrującej, którą teraz znamy pod nazwą Lorenz.

To była fantastyczna *zmiana sił* i na początku 1942 Laboratoria Badawcze Urzędu Pocztowego (Post Office Research Labs) w Dollis Hill zostały poproszone o wyprodukowanie implementacji sieci logicznej rozpracowanej przez Billa Tutte'a. Frank Morrel wyprodukował szafę z przełącznikami krokowymi i przekaźnikami, które symulowały tę sieć. Nazwaną ją "Tunny" (tuńczyk). Więc teraz, gdy ręczni łamacze kodów w Testery pracowicie rozpracowali ustawienia użyte dla określonej wiadomości, to ustawienia te wprowadzano do Tunny i szyfr stawał się czytelny. Jeśli łamaczom kodów

udało się, tekst był w języku niemieckim. Lecz rozpracowanie ustawień zajmowało od czterech do sześciu tygodni. Oznaczało to, że chociaż udowodnili techniczną możliwość złamania kodu Tunny, to w czasie, gdy dana wiadomość została rozszyfrowana, zawarte w niej informacje były zbyt stare, aby przydawały się w działaniach wojennych.



Zarys struktury maszyny szyfrującej Lorenz



Maszyna Tunny - Tuńczyk